



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/649,678	08/28/2003	Natsume Matsuzaki	2003_1213A	5671

513 7590 11/13/2006

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER

ALMEIDA, DEVIN E

ART UNIT PAPER NUMBER

2132

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/649,678

Applicant(s)

MATSUZAKI ET AL.

Examiner

Devin Almeida

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 May 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-68 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-68 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 3/10/2004 5/05/2004 8/09/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 5/28/2003. Claims 1-68 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1-68 are under consideration.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 3/10/2004, 5/05/2004, and 8/09/2004 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 7, 10, 11, 13-15, 17-19, 23, 28 and 29 are rejected under 35 U.S.C. 102(b) as being anticipated by Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 1, Yang teaches a group

Art Unit: 2132

formation/management system, comprising: one or more registered member devices operable to hold common secret information unique to a group; a new member device operable to transmit a request for registration to the group, and to receive and hold the common secret information; and a group management device operable to receive the registration request from the new member device, and when a registered number of member devices is less than a maximum number of member devices registerable in the group, to register the new member device and output the common secret information to the new member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 2, a group formation/management system, comprising: a member device operable to transmit a request for registration to a group, and to receive and hold common secret information unique to the group; and a group management device operable to receive the registration request from the member device, and when a registered number of member devices is less than a maximum number of member devices registerable in the group, to register the member device and output the common secret information to the member device, wherein in an initial state, the group has no member devices registered therein (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to

register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 7, a generating unit operable to generate the common secret information, wherein the communication unit outputs the generated common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 10, the maximum number is formed from a first maximum number and a second maximum number, and the judging unit judges whether the registered number is less than one of the first maximum number and the second maximum number, and registers the member device when judged in the affirmative (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 11, the first maximum number is the number of member devices, out of the maximum number, connectable to the group management device, and the second maximum number is the number of member devices, out of the maximum number, not connectable to the group management device, and the judging unit judges, (i) when the member device is connectable to the group management device, whether the registered number of connectable member devices is less than the first maximum number, and (ii) when the member device is not connectable to the group management device, whether the registered number of non-connectable member

Art Unit: 2132

devices is less than the second maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 13, the judging unit functions to resist invalid access from outside, and the maximum number and the common secret information are stored in an area that is unreadable/unwritable from outside (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 14, the judging unit is included in a portable module that is mountable in the group management device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 15, the judging unit stores a remaining number obtained by subtracting the registered number from the maximum number, and on receipt by the reception unit of the registration request, judges whether the remaining number is "0", and when judged that the remaining number is not "0", the communication unit outputs the common secret information to the member device and the judging unit subtracts "1" from the remaining number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 17, the judging unit, when judged that the registered number is less than the maximum number, issues information showing a valid period during which use of the common secret information is permitted in the member device, increases the registered number, monitors the elapse of the valid period, and reduces the registered number when the valid period ends, and the communication unit outputs the issued information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 18, the judging unit receives from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the received number, and sets the received number as the maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 19, the judging unit newly acquires from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the acquired number, and adds the acquired number to the maximum number to obtain a new maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 23, the communication unit stores therein the common secret information, newly receives a different piece of common secret information, overwrites the stored common secret information with the newly received common secret information, and outputs, regularly or irregularly, the newly received common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 28, the received registration request requests the registration of a predetermined number of other member devices, the judging unit judges whether an aggregate number obtained by adding the predetermined number to the registered number is less than the maximum number, and when judged in the affirmative, generates a permission right permitting a copying of the common secret information to the predetermined number of member devices, and the permission right

is attached to the outputted common secret information (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 29, the received registration request includes a first identifier unique to the member device, the judging unit stores therein the first identifier, the reception unit, after the outputting of the common secret information, receives a second identifier unique to the member device, the judging unit judges whether the second identifier matches the first identifier, and the communication unit, when judged that the first and second identifiers match, again outputs the common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

Claims 3- 6, 35-39, 42, 45, 46, 53, 54, and 59 are rejected under 35 U.S.C. 102(b) as being anticipated by Wong et al: "Keystone: A Group Key Management Service". Wong teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 4, the judging unit includes: an authentication subunit operable to hold a second initial value, and to authenticate the member device, using the second initial value and a first initial value held by the member device; and a device-number judging subunit operable, when authentication is successful, to judge whether the registered number is less than the maximum number, the common secret information outputted by the communication unit shows "registered in the group", and the member device receives and holds the outputted common secret information, and deactivates the first initial value (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 5, the first and second initial values show "unregistered in the group" (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 6, the first and second initial values show "unregistered in any group" (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 35, a member device that uses a content after registering in a group managed by a group management device, comprising: a requesting unit operable to request the group management device for registration to the group; a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information unique to the group; and a holding unit operable to hold the received common secret information (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 36, the holding unit holds a first initial value, the receiving unit is authenticated by the group management device using the first initial value, and receives the common secret information from the group management device when

authentication is successful, and the holding unit deactivates the first initial value and holds the received common secret information (see Wong Chapters 1, 3.1 3.2, 3.3, 4)..

With respect to claim 37, the first initial value shows "unregistered in the group" (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 38, the first initial value shows "unregistered in any group" (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 39, the holding unit overwrites the first initial value with the common secret information (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 42, the receiving unit, after the holding of the common secret information, newly receives a different piece of common secret information from the group management device, and the holding unit overwrites the held common secret information with the newly received common secret information (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 45, the storage subunit is a recording medium mountable in the member device (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 46, an authentication unit operable, after the holding of the common secret information, and when the member device communicates with another member device, to authenticate the other member device using the held common secret information and common secret information held by the other member device (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 53, the holding unit holds a maximum holdable number, which is the number of pieces of common secret information holdable by the holding

unit, and the requesting unit requests the group management device for registration to the group when the number of pieces of held common secret information is less than the maximum holdable number (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 54, holding unit holds identifiers that each identify a different group, the registration request includes one of the identifiers, and the holding unit holds the received common secret information in correspondence with the identifier included in the registration request (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

With respect to claim 59, the receiving unit, after the holding of the common secret information, newly receives a different piece of common secret information from one of the group management device and another group management device, and the holding unit deactivates the held common secret information and holds the newly received common secret information (see Wong Chapters 1, 3.1 3.2, 3.3, 4).

Claims 3, 8-9, 35 and 60-61 are rejected under 35 U.S.C. 102(b) as being anticipated by Steiner et al: "Cliques: A New approach to Group Key Agreement". Steiner teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the

affirmative, to output to the member device, common secret information unique to the group (see Steiner chapters 2, 3, and 5.2).

With respect to claim 8, the common secret information is generated by a management device outside of the group, the judging unit receives the common secret information from the out-group management device, and the communication unit outputs the received common secret information to the member device (see Steiner chapters 2, 3, and 5.2).

With respect to claim 9, the reception unit, on receipt of the registration request, notifies the receipt to a management device outside of the group, the out-group management device judges whether the registered number is less than the maximum number, the judging unit, instead of judging whether the registered number is less than the maximum number, receives a judgment result from the out-group management device, and the communication unit outputs the common secret information to the member device, when the judgment result shows that the registered number is less than the maximum number (see Steiner chapters 2, 3, and 5.2).

With respect to claim 35, a member device that uses a content after registering in a group managed by a group management device, comprising: a requesting unit operable to request the group management device for registration to the group; a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information unique to the group; and a holding unit operable to hold the received common secret information (see Steiner chapters 2, 3, and 5.2).

With respect to claim 61, a dividing unit operable, after the holding of the common secret information, and when the member device is determined by the group management device to be another group management device, to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device; and a communication unit operable to output to the member devices to be registered in the other group, common secret information unique to the other group (see Steiner chapters 2, 3, and 5.2).

With respect to claim 61, the member devices registered in the group each have a priority level, the receiving unit acquires the priority levels of the other member devices, and the dividing unit conducts the dividing based on the acquired priority levels (see Steiner chapters 2, 3, and 5.2).

Claims 3 and 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Paolo (UK Patent application GB 2343025). Paolo teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable,

when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group (see Paolo Figure 3 and page 1 line 6 – page 5 line 29).

With respect to claim 12, the communication unit outputs to another group management device, a request inquiring whether the member device is registerable in the other group management device, the other group management device receives the inquiry request, judges whether a registered number of member devices is less than a maximum number of member devices registerable with the other group management device, and when judged in the affirmative, registers the member device and outputs the common secret information to the group management device, and the communication unit, on receipt of the common secret information from the other group management device, outputs the received common secret information to the member device (see Paolo Figure 3 and page 1 line 6 – page 5 line 29).

Claims 3 and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Canetti et al: "Multicast Security: A Taxonomy and Some Efficient Construction". Canetti teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a

Art Unit: 2132

communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group (see Canetti see chapter 4).

With respect to claim 16, the reception unit, after the outputting of the common secret information, receives from the member device, a request for withdrawal from the group, the communication unit, on receipt by the reception unit of the withdrawal request, outputs to the member device, a notification indicating to delete the common secret information, the reception unit receives from the member device, a notification showing that deletion of the common secret information has been completed, and the judging unit, on receipt by the reception unit of the deletion-completed notification, reduces the registered number (see Canetti see chapter 4 i.e. deletion of group key).

Claims 3, 20-22, 24-27, 34, 43, 51 and 66-68 are rejected under 35 U.S.C. 102(b) as being anticipated by Yevgeny (UK Patent application GB 2353682). Yevgeny teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the

affirmative, to output to the member device, common secret information unique to the group (see Yevgeny page 5 lines 11-16).

With respect to claim 20, the reception unit, after the outputting of the common secret information, receives a communication request from the member device, the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and the communication unit communicates with the member device when authentication is successful (see Yevgeny page 5 lines 11-16).

With respect to claim 21, a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; and an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key, wherein the communication unit outputs the encrypted content and the encrypted content key to the member device (see Yevgeny page 5 lines 11-16).

With respect to claim 22, the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and shares a session key with the member device, using the common secret information, and the encryption unit, when authentication is successful, encrypts the content key using the shared session key (see Yevgeny page 5 lines 11-16).

With respect to claim 24, a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; an encryption unit operable to encrypt the content key using a key generated based on the common

secret information, to generate an encrypted content key; and a writing unit operable to write the encrypted content and the encrypted content key to a portable recordable medium (see Yevgeny page 5 lines 11-16).

With respect to claim 25, the received registration request includes an identifier identifying the member device, and the encryption unit encrypts the content key using a key generated based on the common secret information and the identifier, to generate the encrypted content key (see Yevgeny page 5 lines 11-16).

With respect to claim 26, the encryption unit encrypts the content key using a key generated based on the common secret information and an identifier unique to the portable recordable medium (see Yevgeny page 5 lines 11-16).

With respect to claim 27, a holding unit operable to hold, in correspondence with identifiers that each identify a different group, (i) common secret information unique to the group and (ii) a maximum number of member devices registerable in the group, wherein the received registration request includes one of the identifiers, the judging unit, on receipt by the reception unit of the registration request, judges whether the number of member devices registered in a group identified by the identifier is less than a maximum number corresponding to the identifier, and when judged in the affirmative, registers the member device in the group and selects common secret information corresponding to the identifier, and the communication unit outputs the selected common secret information to the member device (see Yevgeny page 5 lines 11-16).

With respect to claim 34, a determining unit operable, after the outputting of the common secret information, to determine a member device registered in the group to be

another group management device; and a dividing unit operable to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device, and the communication unit outputs, after the dividing by the dividing unit, a different piece of common secret information to the member devices to be registered in the group managed by the group management device (see Yevgeny page 5 lines 11-16).

With respect to claim 43, the requesting unit requests the group management device for delivery of the content, the receiving unit receives from the group management device, an encrypted content generated by encrypting the content using a content key, and an encrypted content key generated by encrypting the content key using an encryption key generated based on the common secret information, and the member device further comprises a decryption unit operable to generate a decryption key the same as the encryption key, based on the common secret information, to decrypt the encrypted content key using the decryption key to obtain a content key, and to decrypt the encrypted content using the content key to obtain a content (see Yevgeny page 5 lines 11-16).

With respect to claim 51, the receiving unit receives from the group management device, an encrypted content encrypted using a content key, and an encrypted content key generated by encrypting the content key using an encryption key generated based on the common secret information, and the member device further comprises: a decryption unit operable to read the common secret information from the mounted

portable module, generate a decryption key the same as the encryption key, based on the read common secret information, decrypt the encrypted content key using the decryption key to obtain a content key, and decrypt the encrypted content using the content key to obtain a content (see Yevgeny page 5 lines 11-16).

With respect to claim 66, an authentication method used in a group management device that manages a group, comprising the steps of: receiving a request from a member device; authenticating whether the member device is a legitimate device, using common secret information unique to the group and common secret information held by the member device; and judging the member device to be registered in the group when authentication is successful (see Yevgeny page 5 lines 11-16).

With respect to claim 67, a computer program used in a group management device that manages a group, comprising the steps of: receiving a request from a member device; authenticating whether the member device is a legitimate device, using common secret information unique to the group and common secret information held by the member device; and judging the member device to be registered in the group when authentication is successful (see Yevgeny page 5 lines 11-16).

With respect to claim 68, a recording medium storing a computer program used in a group management device that manages a group, the computer program comprising the steps of: receiving a request from a member device; authenticating whether the member device is a legitimate device, using common secret information unique to the group and common secret information held by the member device; and

judging the member device to be registered in the group when authentication is successful (see Yevgeny page 5 lines 11-16).

Claims 3 and 30-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Huang et al: "Group leader election under-state routing". Huang teaches everything with respect to claim 3, a group management device that manages a group, comprising: a reception unit operable to receive from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group (see Huang chapter 2.2).

With respect to claim 30, when the group management device is determined to be a new group management device for managing a new group formed by combining groups managed by a plurality of group management devices, the communication unit outputs to member devices registered in the groups, new common secret information unique to the new group, and when one of the other group management devices is determined to be the new group management device, the group management device further comprises: a receiving unit operable to receive the new common secret information from the other group management device; and a holding unit operable to hold the received new common secret information (see Huang chapter 2.2).

With respect to claim 31, the communication unit determines in conjunction with the other group management devices, one of the group management devices to be the new group management device (see Huang chapter 2.2).

With respect to claim 32, the holding unit stores therein a priority level of the group management device, and the communication unit determines, out of the stored priority level and priority levels of the other group management devices, the group management device having the highest priority level to be the new group management device (see Huang chapter 2.2).

With respect to claim 33, each member device registered in the groups managed by the group management device and the other group management devices has a priority level, and when the group management device is determined to be the new group management device, the reception unit acquires the priority levels of the member devices, the group management device further comprises a selecting unit operable to select, in order from highest to lowest of the acquired priority levels, member devices for registration in the new group, the selected number of member devices being less than or equal to a maximum number of member devices registerable in the new group, and the communication unit outputs the new common secret information to the selected member devices (see Huang chapter 2.2).

Claims 35, 40, 41, 44, 47-50, 52, 55, 56 and 62-64 are rejected under 35 U.S.C. 102(b) as being anticipated by Peinado (U.S. Patent Application Publication # 2002-0013772). Peinado teaches everything with respect to claim 35, a member device

Art Unit: 2132

that uses a content after registering in a group managed by a group management device, comprising: a requesting unit operable to request the group management device for registration to the group; a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information unique to the group; and a holding unit operable to hold the received common secret information (see Peinado, paragraph 0285-0326).

With respect to claim 40, a communication unit operable, after the holding of the common secret information, to output the common secret information to another member device; and a deletion unit operable to delete the held common secret information after the outputting by the communication unit, wherein the holding unit reactivates the first initial value after the deleting by the deletion unit (see Peinado, paragraph 0285-0326).

With respect to claim 41, the requesting unit requests the group management device for withdrawal from the group, the receiving unit receives from the group management device, a notification indicating to delete the common secret information, and the holding unit deletes the held common secret information and reactivates the first initial value (see Peinado, paragraph 0285-0326).

With respect to claim 44, the holding unit includes a storage subunit that is unreadable/unwritable from outside, and the storage subunit stores therein the received common secret information (see Peinado, paragraph 0285-0326).

With respect to claim 47, a communication unit operable, after the holding of the common secret information, to output the common secret information to another

member device; and a deletion unit operable to delete the held common secret information after the outputting by the communication unit (see Peinado, paragraph 0285-0326).

With respect to claim 48, the requesting unit requests the group management device for withdrawal from the group, the receiving unit receives from the group management device, a notification indicating to delete the common secret information, and the holding unit, on acquisition of the deletion notification by the receiving unit, deletes the held common secret information (see Peinado, paragraph 0285-0326).

With respect to claim 49, the received common secret information includes information showing a valid period during which use of the common secret information is permitted in the member device, and the holding unit monitors an elapse of the valid period and deletes the common secret information when the valid period ends (see Peinado, paragraph 0285-0326).

With respect to claim 50, the requesting, receiving and holding units are included in a portable module that is mountable in the member device and the group management device, and the receiving unit receives the common secret information from the group management device, when the portable module is mounted in the group management device (see Peinado, paragraph 0285-0326).

With respect to claim 52, the portable module further includes: a notifying unit operable, when the portable module is mounted in the member device, to notify the held common secret information to the member device; and a management unit operable, after the notifying of the held common secret information, to prohibit the notifying unit

from again notifying the held common secret information to the member device, and the member device further comprises a storage unit operable to receive and store therein the common secret information notified from the portable module (see Peinado, paragraph 0285-0326).

With respect to claim 55, the requesting unit requests the group management device for registration of a predetermined number of other member devices, the received common secret information has attached a permission right permitting a copying of the common secret information to the predetermined number of member devices, the member device further comprises a communication unit operable to output the common secret information to another member device, and the holding unit reduces the number of copies permitted by the permission right by "1" when the common secret information is outputted by the communication unit (see Peinado, paragraph 0285-0326).

With respect to claim 56, the holding unit holds an identifier unique to the member device, the communication unit acquires from the other member device, an identifier unique to the other member device, and the requesting unit transmits the held and acquired identifiers to the group management device (see Peinado, paragraph 0285-0326).

With respect to claim 62, a registration device that registers a member device in a group managed by a group management device, comprising: a holding unit operable to receive from the group management device and hold, common secret information unique to the group; and a notifying unit operable, when the registration device is

connected to the member device, to notify the common secret information to the member device (see Peinado, paragraph 0285-0326).

With respect to claim 63, a management unit operable, after the notifying of the common secret information, to prohibit the notifying unit from again notifying the common secret information to the member device (see Peinado, paragraph 0285-0326).

With respect to claim 64, a reception unit operable to receive from the member device, a request for acquisition of the common secret information, wherein the notifying unit notifies the common secret information to the member device when the acquisition request is received by the reception unit (see Peinado, paragraph 0285-0326).

Claim 65 is rejected under 35 U.S.C. 102(b) as being anticipated by Setia et al: "Kronos a Scalable Group Re-keying Approach for Secure Multicast". Setia teaches everything with respect to claim 65, a member device that uses a content after registering in a group managed by a group management device, comprising: a selecting unit operable to select one of a plurality of group management devices based a preset criterion; a requesting unit operable to request the selected group management device for registration to a group; a receiving unit operable to receive, from the selected group management device, common secret information unique to the group; and a holding unit operable to hold the received common secret information, wherein the preset criterion is, with respect to each group management device, one of (i) a distance from the member device, (ii) a communication time with the member device, (iii) a processing capacity, and (iv) a processing state (see Setia chapters 3.1, 3.2, 4.1, and 4.3 i.e.

impact of increasing processing power, and the impact of manager location n lolus and Kronos).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 57 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al: "Keystone: A Group Key Management Service" in view of Mason (U.S. Patent # 6,158,004). Wong teaches everything with respect to claim 35 above but with respect to claim 57, does not teach the holding unit holds an identifier unique to the member device, the registration request includes the identifier, the holding unit, on receipt of a power-OFF instruction, deletes the held common secret information and sets power off, and on receipt of a power-ON instruction, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group management device. Mason teaches the holding unit holds an identifier unique to the member device, the registration request includes the identifier, the holding unit, on receipt of a power-OFF instruction, deletes the held common secret information and sets power off, and on receipt of a power-ON instruction, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group

management device (see Mason column 6 line 60 – column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have deleted the common secret during the power-off to ensure the high security. Therefore one would have been motivated to have deleted the common secret during the power-off.

Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al: "Keystone: A Group Key Management Service" in view of Hornbuckle (U.S. Patent # 5,649, 187). Wong teaches everything with respect to claim 35 above but with respect to claim 58, does not teach the holding unit holds an identifier unique to the member device, the registration request includes the identifier, the holding unit, when communication with the group management device is interrupted, deletes the held common secret information, and when communication with the group management device is reestablished, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group management device. Hornbuckle teaches, the holding unit holds an identifier unique to the member device, the registration request includes the identifier, the holding unit, when communication with the group management device is interrupted, deletes the held common secret information, and when communication with the group management device is reestablished, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group management device (see Hornbuckle column 13

lines 4-41). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have deleted the common secret during the power-off and make the device request a new common secret from the group management device to ensure the high security. Therefore one would have been motivated to have deleted the common secret during the power-off and make the device request a new common secret to increase security.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

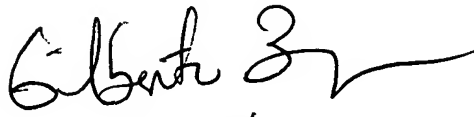
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

Art Unit: 2132

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA
Devin Almeida
Patent Examiner
11/08/2006


GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100